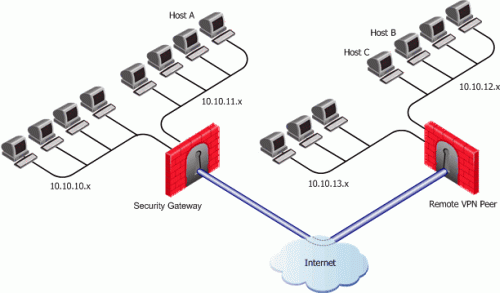
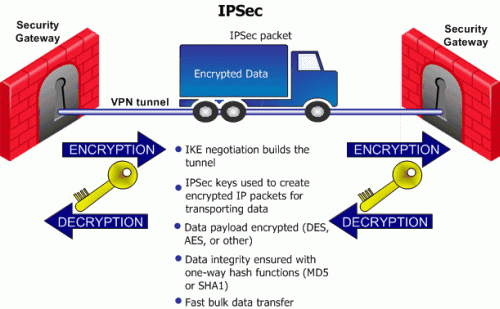
**IPSEC**

IPsec es un protocolo **IETF (Internet Engineering Task Forte**) que define la forma en que se puede configurar una VPN de manera segura mediante el protocolo de Internet.



*Figura 1: VPN*



*Figura 2: Funcionamiento de IPSec*

1. **SUB-PROTOCOLOS DE IPSEC**
   1. **Encapsulated Security Payload (ESP)**

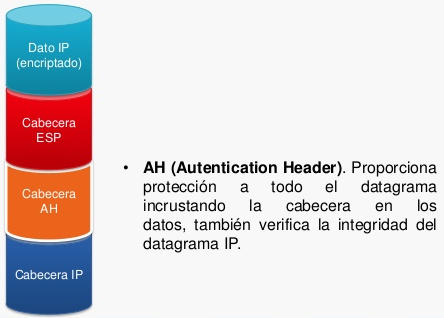
Es un protocolo de seguridad que proporciona confidencialidad y autenticación mediante el cifrado del paquete IP. El cifrado de paquetes IP oculta los datos y las identidades del origen y el destino. ESP autentica el paquete IP y el encabezado ESP internos. La autenticación proporciona la autenticación del origen de los datos y la integridad de los datos. Si bien el cifrado y la autenticación son optativos en ESP, se debe seleccionar, como mínimo, uno de ellos.



*Figura 3: Cabecera ESP*

* 1. **Authentication Header (AH)**

Es el protocolo que se debe utilizar cuando no se requiere o no se permite la confidencialidad. Proporciona la autenticación y la integridad de datos para los paquetes IP que se transmiten entre dos sistemas. Sin embargo, AH no proporciona la confidencialidad (el cifrado) de datos de los paquetes. Todo el texto se transporta como texto no cifrado. Cuando se utiliza solo, el protocolo AH proporciona una protección poco eficaz.



*Figura 4: Cabera AH*

1. **SERVICIOS IPSec**

Los servicios de seguridad IPsec proporcionan cuatro funciones fundamentales, las cuales se muestran en la ilustración:

* 1. **Confidencialidad (cifrado):** en una implementación de VPN, los datos privados se transfieren a través de una red pública. Por este motivo, la confidencialidad de los datos es fundamental. Esto se puede lograr mediante el cifrado de los datos antes de transmitirlos a través de la red. Este es el proceso de tomar todos los datos que una computadora envía a otra y codificarlos de una manera que solo la otra computadora pueda decodificar. Si se intercepta la comunicación, el pirata informático no puede leer los datos. IPsec proporciona características de seguridad mejoradas, como algoritmos de cifrado seguros.
  2. **Integridad de datos:** el receptor puede verificar que los datos se hayan transmitido a través de Internet sin sufrir ningún tipo de modificaciones ni alteraciones. Si bien es importante que los datos a través de una red pública estén cifrados, también es importante verificar que no se hayan modificado cuando estaban en tránsito. IPsec cuenta con un mecanismo para asegurarse de que la porción cifrada del paquete, o todo el encabezado y la porción de datos del paquete, no se haya modificado. IPsec asegura la integridad de los datos mediante checksums, que es una comprobación de redundancia simple. Si se detecta una alteración, el paquete se descarta.
  3. **Autenticación:** verifica la identidad del origen de los datos que se envían. Esto es necesario para la protección contra distintos ataques que dependen de la suplantación de identidad del emisor. La autenticación asegura que se cree una conexión con el compañero de comunicación deseado. El receptor puede autenticar el origen del paquete mediante la certificación del origen de la información. IPsec utiliza el intercambio de claves de Internet (IKE) para autenticar a los usuarios y dispositivos que pueden llevar a cabo la comunicación de manera independiente. IKE utiliza varios tipos de autenticación, por ejemplo, nombre de usuario y contraseña, contraseña por única vez, biometría, clave previamente compartida (PSK) y certificados digitales.
  4. **Protección antirreproducción:** es la capacidad de detectar y rechazar los paquetes reproducidos, y ayuda a prevenir la suplantación de identidad. La protección antirreproducción verifica que cada paquete sea único y no esté duplicado. Los paquetes IPsec se protegen mediante la comparación del número de secuencia de los paquetes recibidos con una ventana deslizante en el host de destino o el gateway de seguridad. Se considera que un paquete que tiene un número de secuencia anterior a la ventana deslizante tiene un retraso o está duplicado. Los paquetes duplicados y con retraso se descartan.